Senate

General Assembly

File No. 455

February Session, 2008

Substitute Senate Bill No. 677

Senate, April 4, 2008

The Committee on Government Administration and Elections reported through SEN. SLOSSBERG of the 14th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT CONCERNING THE USE OF STATE MOBILE COMPUTING AND STORAGE DEVICES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective from passage*) (a) For the purposes of this section, (1) "confidential or restricted state data" means personally identifiable information that is not in the public domain and, if improperly disclosed, could be used to steal an individual's identity, violate an individual's right to privacy or otherwise harm an individual. Such data includes, but is not limited to, organizational information that is not in the public domain and, if improperly disclosed, might cause a significant or severe degradation in mission capability, result in significant or major damage to organizational assets, result in significant or major financial loss, or result in significant, severe or catastrophic harm to individuals; (2) "mobile computing devices" means any portable or mobile computing and telecommunications devices that can execute programs; (3) "mobile storage devices" means mobile computing devices, diskettes, magnetic

tapes, external or removable hard drives, flash cards, thumb drives, jump drives, compact disks and digital video disks; (4) "secure mobile device" means a mobile computing or storage device that has a sufficient level of access control, protection from malware and strong encryption capabilities to ensure the protection and privacy of state data that may be stored on such mobile computing or storage device; and (5) "users" means all executive branch agencies and employees, whether permanent or nonpermanent, full or part-time, and all consultants or contracted individuals retained by an executive branch agency with access to state data.

(b) There is established a policy on security for mobile computing and storage devices, as described in this section. Such policy shall apply to all users.

(c) No confidential or restricted state data shall reside on any mobile device, except as set forth in subsection (d) of this section. Each executive branch state agency shall utilize secure remote data access methods, as approved by the Department of Information Technology, in support of mobile users.

(d) In the event that utilization of secure remote access methods is not possible, the executive branch agency shall adhere to the following restrictions and requirements: (1) Such agency head shall authorize and certify in writing to the Chief Information Officer, in advance, that the storing of restricted and confidential state data on the mobile device is necessary to conduct agency business operations; (2) the agency head, or the agency head's designee, shall determine and certify in writing to the Chief Information Officer that reasonable alternative means to provide the user with secure access to such state data do not exist; (3) such agency head, or such agency head's designee, shall assess the sensitivity of the data to reside on a secure mobile device and determine that the business need necessitating storage on the mobile device outweighs the associated risks of loss or compromise; and (4) such agency head, or such agency head's designee, shall authorize, in writing, the storage of specific state data

on a secure mobile device and the acceptance of all associated risks.

(e) State data that an executive branch agency head has authorized to be stored on a secure mobile device, pursuant to subsection (d) of this section, shall be: (1) The minimum data necessary to perform the business function necessitating storage on the mobile device; (2) stored only for the time needed to perform the business function; (3) encrypted using methods authorized by the Department of Information Technology; (4) protected from any and all forms of unauthorized access and disclosure; and (5) stored only on secure mobile devices in accordance with Department of Information and Technology policies, standards and guidelines.

(f) Any state data placed on a mobile device shall be documented, tracked and audited by the authorizing executive branch agency. The information tracked shall include: (1) The identification of the individual authorizing storage of the data on the mobile device; (2) the authorized user of the mobile device; (3) the asset tag of the mobile device; (4) information about the stored data; and (5) the final disposition of such data.

(g) Executive branch agencies shall configure mobile devices to allow only the minimum features, functions and services needed to carry out agency business requirements.

(h) Executive branch agencies shall ensure that mobile computing devices are configured with approved and properly updated software-based security mechanisms including anti-virus, anti-spyware, firewalls and intrusion detection. Users shall not bypass or disable such security mechanisms under any circumstances.

(i) Users in the possession of state-owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas shall not leave such devices unattended at any time, and shall take all reasonable and appropriate precautions to protect and control such devices from unauthorized physical access, tampering, loss or theft.

(j) Executive branch agencies shall establish and document reporting, mitigation and remediation procedures for lost or stolen mobile devices containing state data and for state data that is compromised through accidental or nonauthorized access or disclosure.

(k) In the event that a mobile device containing state data is lost, stolen or misplaced or the user has determined unauthorized access has occurred, the user shall immediately notify his or her agency of the incident. The affected agency shall immediately notify the Department of Information Technology Help Desk of the incident in order to initiate effective and timely response and remediation.

(l) Executive branch agencies shall develop and implement a formal, documented security awareness and training program sufficient to ensure compliance with the policy set forth in this section.

(m) Executive branch agencies shall obtain a signed, formal acknowledgement from users indicating that they have understood and agreed to abide by the provisions of the policy set forth in this section.

(n) All executive branch agencies and users shall comply with the policy set forth in this section and any associated procedures.

(o) In accordance with the state Network Security Policies and Procedures, each executive branch agency shall be responsible for the assessment and categorization of such agency's data as confidential or restricted.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*from passage*	New section

GAE *Joint Favorable Subst.*

The following fiscal impact statement and bill analysis are prepared for the benefit of members of the General Assembly, solely for the purpose of information, summarization, and explanation, and do not represent the intent of the General Assembly or either chamber thereof for any purpose:

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 09 $	FY 10 $
Department of Information Technology	GF - None	None	None
All	App Fund - None	None	None

Note: GF=General Fund; App Fund=All Appropriated Funds

Municipal Impact: None

Explanation

The bill has no fiscal impact because the bill formalizes current practice to statute.

The Out Years

There is no annualized fiscal impact.

OLR Bill Analysis

sSB 677

AN ACT CONCERNING THE USE OF STATE MOBILE COMPUTING AND STORAGE DEVICES.

SUMMARY:

This bill codifies the Department of Information Technology's (DOIT) existing security policy on mobile computing and storage devices for executive branch agencies and employees, including consultants and contractors with access to state data (see BACKGROUND). Generally, it bans the storage of confidential or restricted state data on a mobile device, but creates an exception to the ban with certain restrictions. The ban does not apply to the legislative or judicial branches.

The bill also (1) establishes requirements for configuring mobile devices; (2) prohibits those who use state-owned mobile devices from leaving them unattended when in a public setting or traveling, among other things; (3) requires agencies to establish procedures for lost or stolen mobile devices, and report any such incident to DOIT; and (4) requires agencies to implement a training program on the security policy and obtain acknowledgement from employees, consultants, and contractors that they will abide by the policy.

The bill specifies that each executive branch agency and employee, and each covered consultant and contractor, must abide by the policy and any associated procedures. (However, the bill does not designate an enforcement authority.) Further, each agency is responsible for assessing and categorizing its data as confidential or restricted in accordance with state "Network Security Policies and Procedures," which DOIT establishes (see BACKGROUND).

EFFECTIVE DATE: Upon passage

APPLICATION

Under the bill, every user of a mobile computing or storage device must abide by the security policy on confidential or restricted state data.

"User" means an executive branch agency or employee (whether full-time, part-time, permanent, or temporary), or an individual with whom an executive branch agency contracts or hires as a consultant who has access to data.

Mobile device means both "mobile computing device" (portable or mobile computing and telecommunications device that can execute programs) and "mobile storage device" (mobile computing device, diskette, magnetic tape, external or removable hard drive, flash card, thumb drive, jump drive, compact disk, or digital video disk).

"Confidential or restricted data" means personally identifiable information that is not in the public domain and, if improperly disclosed, could be used to steal an individual's identity, violate his or her privacy, or otherwise cause harm. It includes organizational information that is not in the public domain and, if improperly disclosed, might cause a significant degradation in mission capability, or result in major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals.

PROHIBITION

The bill generally bans the storage of confidential or restricted state data on any mobile device. It instead requires executive branch agencies to use "secure remote data access methods" which DOIT approves, to support mobile users.

EXCEPTION

The bill creates an exception to the ban, allowing the storage of confidential or restricted state data on a mobile device if it is not possible to utilize a secure remote access method. In that case, the bill

places certain restrictions and requirements on the agency with respect to the data and maintaining its security.

First, the agency head must authorize and certify in writing to DOIT's chief information officer, in advance, that storing restricted or confidential state data on a mobile device is necessary to conduct the agency's business. Then the agency head or his or her designee must (1) determine and certify in writing to the chief information officer that reasonable alternatives do not exist to provide the user with secure access to the necessary data; (2) assess the data's sensitivity and determine that the business need for storing it on the mobile device outweighs the risks associated with losing or compromising it; and (3) authorize, in writing, the storage of specific data on a secure mobile device and acceptance of all associated risks.

A "secure mobile device" is a mobile computing or storage device that has a sufficient level of access control, protection from malware, and strong encryption capabilities to ensure the protection and privacy of state data that may be stored on it.

Restrictions

Within the exception, any state data that an executive branch agency authorizes for storage on a secure mobile device must be:

1. the minimum data necessary to perform the business function;
2. stored only as long as needed to perform the business function;
3. encrypted using DOIT-authorized methods; and
4. protected from any and all forms of unauthorized access and disclosure.

In addition, the bill stipulates that such state data be stored on secure mobile devices and in accordance with DOIT's policies, standards, and guidelines only.

Each executive branch agency must document, track, and audit any

data it authorizes for placement on a mobile device. The bill requires the tracked information to include (1) the identity of the individual who authorizes the storage, (2) the authorized user, (3) the mobile device's asset tag, (4) information about the stored data, and (5) the final disposition of the data.

MOBILE DEVICE REQUIREMENTS

Executive branch agencies must configure mobile devices to allow only the minimum features, functions, and services needed to carry out their required business. They must configure mobile computing devices, in particular, with approved and properly updated software-based security mechanisms, including anti-virus, anti-spyware, firewalls, and intrusion detection.

USER REQUIREMENTS

The bill bans users from bypassing or disabling a mobile computing device's security mechanisms under any circumstances. It additionally prohibits users who travel with state-owned mobile devices, or bring them to pubic places such as a meeting room or other unprotected area, from leaving them unattended at any time. Any user who transports a state-owned mobile device to such a location must take all reasonable and appropriate precautions to protect and control the device from unauthorized physical access, tampering, loss, or theft.

LOST OR STOLEN MOBILE DEVICES

Executive branch agencies must establish and document reporting, mitigation, and remediation procedures for lost or stolen mobile devices containing any state data. Agencies must also establish and document such procedures for state data that is compromised through accidental or unauthorized access or disclosure.

If a mobile device containing state data is lost, stolen, or misplaced, or if the user determines that unauthorized access has occurred, the user must immediately notify his or her agency of the incident. The agency must immediately notify DOIT's Help Desk.

TRAINING AND USER AUTHORIZATIONS

The bill requires each executive branch agency to develop and implement a formal, documented security awareness and training program. The program must be sufficient to ensure compliance with the bill's security policy.

In addition, agencies must obtain a signed, formal acknowledgement from each user indicating that they understand and agree to the security policy.

BACKGROUND

Policy on Security for Mobile Computing and Storage Devices

DOIT's Chief Information Officer established the "Policy on Security for Mobile Computing and Storage Devices," effective September 10, 2007, to protect state data that is stored on mobile devices. The policy refers to and supplements the "State of Connecticut Network Security Policy and Procedures."

Network Security Policies and Procedures

Under these policies and procedures, each agency must determine what agency information is confidential or restricted, and submit this information to DOIT in writing.

Related Bills

The General Law Committee reported three bills related to identity theft:

sSB 30 (File 126) broadens the definition of "identity theft" as it is used under the state's penal code; allows identity theft victims to sue for damages those who traffic in personal identifying information; requires, rather than allows, courts to issue orders to correct the public record whenever a person is convicted of identity theft; prohibits employers from disclosing their employees' Social Security numbers without consent; makes the illegal proceeds of identity theft crimes subject to forfeiture; requires financial institutions to take steps to protect against identity theft; and creates an account to reimburse people hurt by the dissemination of their personal identifying

information.

sHB 5658 (File 145) prohibits people, businesses, and other organizations, other than the state and its political subdivisions, from requesting Social Security numbers as a condition of leasing, purchasing, or receiving products, goods, or services.

sHB 5760 (File 147) makes a state agency, person, or business that loses or discloses an individual's personal identifying information responsible for identity theft monitoring and protection costs and any other costs or fees if the individual's identity is stolen.

The Judiciary Committee reported sSB 671, which requires governmental entities to make certain disclosures when requesting Social Security numbers and requires people, businesses, and governmental entities that lose, or cause the unauthorized disclosure of, a person's Social Security number to notify him or her and pay for identity theft monitoring protection if requested, among other things.

COMMITTEE ACTION

Government Administration and Elections Committee

Joint Favorable Substitute
Yea 13 Nay 0 (03/17/2008)